UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

ALISON WILLIAMSON individually and on behalf of all others similarly situated, Plaintiff, v. AT&T, INC., Defendant.	Case No. 3:24-cv-00790 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Alison Williamson ("Plaintiff"), individually, and on behalf of all others similarly situated, bring this action against AT&T Inc. ("Defendant" or "AT&T"). Plaintiff bring this action by and through her attorneys, and alleges, based upon personal knowledge as to her own actions, and based upon information, belief, and reasonable investigation by her counsel as to all other matters, as follows.

I. INTRODUCTION

"We take cybersecurity very seriously and privacy is a fundamental commitment at AT&T."

1. Despite unctuous privacy assurances, AT&T has suffered one of the largest and most consequential data breaches in U.S. history, compromising the sensitive personal information of approximately 73 million consumers. Initial indications of a hacking involving AT&T customers was rumored back in 2021, yet Defendant was only recently forced to acknowledged that certain former and current account holder information was exfiltrated when it was determined that the information was released on the dark web.

2. Plaintiff now brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII" or "Private Information")[1] including, but not limited to full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, AT&T account numbers and passcodes.[2]

3. Defendant provides more than 100 million U.S. consumers with communications across mobile and broadband. It uses a variety of platforms to provide broadband connectivity, including higher speeds made possible by its extensive fiber and wireless network.

4. Defendant is an American multinational telecommunications holding company headquartered in downtown Dallas, Texas. It is currently the world's fourth largest telecommunications company by revenue and the largest wireless carrier in the United States with annual worldwide revenues of nearly $118 billion in 2023, placing it 13th on the Fortune 500 rankings. AT&T's wireless 5G network covers around 295 million people across the United States.

5. To provide these telecommunication services, and in the ordinary course of AT&T's business, it acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and Class Members' PII.

6. With this action, Plaintiff seeks to hold Defendant accountable for the harms it caused and will continue to cause Plaintiff and at least 7.6 million current and approximately 65.4 million former AT&T account holders that have been impacted and other similarly situated

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] Keeping Your Account Secure, https://www.att.com/support/article/myaccount/000101995?bypasscache=1 (last visited April 2, 2024).

individuals in the massive and preventable cyberattack purportedly discovered by Defendant, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive PII of Plaintiff and Class Members which was inadequately maintained by Defendant ("Data Breach").[3]

7. Plaintiff further seeks to hold Defendant responsible for not ensuring that Plaintiff's PII was maintained and secured in a manner consistent with industry standards.

8. On or about March 30, 2024, AT&T informed many of its account holders and former account holders, including Class Members by email notice and mail notice that their sensitive PII had been compromised ("Notice Letter").

9. Defendant has also confirmed that Plaintiff's and Class Members' PII was released on the Dark Web. "AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web….which includes personal information such as social security numbers, the source of the data is still being assessed."[4]

10. Upon information and belief, the Data Breach occurred in 2019 but Defendant did not begin informing victims of the Data Breach until March 30, 2024, approximately five years later. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they received Notice Letters from Defendant. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at and imminent and significant risk of identity theft, along with other forms of personal, social, and financial harm.

---

[3] *Id.*; *see also AT&T Forced to Reset Millions of Account Passcodes After Hacked Data Spreads Online*, Inc.com, April 1, 2024, https://www.inc.com/kit-eaton/att-forced-to-reset-millions-of account-passcodes-after-hacked-data-spreads-online.html.

[4] *Keeping Your Account Secure*, https://www.att.com/support/article/myaccount/ 000101995?bypasscache=1 (last visited April 1, 2024).

11. The Notice Letter provides no further information regarding the Data Breach and only recommends that victims such as Plaintiff, reset their passwords, monitor their account activity, and potentially place fraud alerts on their accounts. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiff's and Class Members' PII remains in the possession of criminals.

12. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' PII for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members' PII in its possession and to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

13. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' PII from a foreseeable cyberattack on its systems or third-party vendor that resulted in the unauthorized access and theft of Plaintiff's and Class Members' PII.

14. Currently, the full extent of the type of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase in the litigation.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiff's and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third-party.

16. Based on the type of sophisticated and targeted criminal activity, the type of PII involved, and Defendant's admission that PII was accessed, it can be concluded that the unauthorized criminal third-party was able to successfully target Plaintiff's and Class Members' PII, including full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, AT&T account numbers and passcodes, for the purposes of utilizing or selling the PHI for use in future fraud and identity theft related cases.

17. As a direct result of Defendant's data security failures and the resulting foreseeable Data Breach, Plaintiff's and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

18. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) uncompensated loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) deprivation of value of their PII; (h) invasion of their privacy; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

19. Accordingly, Plaintiff bring this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiff's and Class Members' PII; its failure to reasonably provide timely notification that Plaintiff's and Class Members' PII had been compromised by an unauthorized third party; and for intentionally and/or negligent unconscionably deceiving Plaintiff and Class Members concerning the status, safety, location, access, and protection of their PII.

II. PARTIES

20. Plaintiff Alison Williamson is an adult individual and, at all relevant times herein, a resident and citizen of the State of Georgia, residing in Fayetteville, Georgia.

21. Defendant AT&T, Inc. is a Texas corporation with its principal place of business located at 208 South Akard Street, Dallas, Texas. Defendant is a citizen of Texas and has a registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

III. JURISDICTION AND VENUE

22. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendant.

23. This Court has general personal jurisdiction over Defendant because Defendant AT&T's principal place of business sis in the Dallas Division of the Northern District of Texas, and conducts business in this District, and the acts and omissions giving rise to the claims alleged herein occurred in and emanated from this District.

24. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas and is being served in this District.

IV. FACTUAL ALLEGATIONS

A. Background

25. Defendant AT&T is an international telecommunications corporation headquartered in Dallas, Texas. AT&T offers mobile communications services and broadband connectivity to millions of resident and business customers throughout the United States.

26. Defendant's Privacy Policy, posted on its website, states that at AT&T "[w]e work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information."[5]

27. Defendant's Privacy Policy also indicates that, "[i]f a breach occurs, we'll notify you as required by law."[6]

28. Defendant's emailed Notice Letter received on or about March 31, 2024 states, "[w]e (AT&T) take cybersecurity very seriously and privacy is a fundamental commitment at AT&T."[7] The emailed Notice Letter also indicates that her information involved in the Data Breach "may have included full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode."

---

[5] *Privacy Policy*, https://about.att.com/privacy/privacy-notice.html (last visited April 2, 2024).
[6] *Id.*
[7] Emailed Notice Letter is the same as Defendant's online notice. *See Keeping Your Account Secure*, https://www.att.com/support/article/myaccount/000101995?bypasscache=1 (last visited April 2, 2024).

29. Indeed, Defendant has made numerous misleading security assurance representations that it would adequately protect Plaintiff's and Class Members' sensitive PII but has subsequently failed to do so.

B. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

30. In the ordinary course of business, Defendant collects and maintains highly sensitive PII of its customers and potential customers, as part of its normal telecommunications business operations.

31. Because of the highly sensitive and personal nature of the PII Defendant acquires and stores with respect to customers, past and present, Defendant promises to keep PII private and secure; comply with industry standards related to data security, inform consumers of its legal duties to comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that relate to business operations and provide adequate notice to individuals if thei rpII is disclosed without authorization.

32. Defendant acquires, collects, stores and maintains Plaintiff's and Class Members' PII and has a duty to protect such highly sensitive PII from unauthorized access.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

34. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII entrusted with Defendant.

35. Plaintiff and Class Members relied on, and reasonably expected Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential

and securely maintained, to use their PII solely for proper business purposes, and to prevent the unauthorized disclosure of their PII.

C. The Cyberattack and Data Breach

36. AT&T detected unauthorized access to certain computer systems within its network environment.[8]

37. AT&T took precautionary measures and reset passcodes, as an extra layer of protection for AT&T accounts.[9]

38. Through its own investigation, AT&T determined that the data of 7.6 million current AT&T account holders and 65.4 million former account holders, including Plaintiff and Class Members, were accessed as part of the cyberattack and have been released on the Dark Web.[10]

D. AT&T Had a Duty and Obligation to Protect Private Information

39. Defendant has an obligation to protect the Private Information belonging to Plaintiff and Class Members. Plaintiff and Class Members had a reasonable expectation that their sensitive PII that was entrusted to Defendant would be protected and safeguarded from unauthorized access or disclosure.

The Data Breach was Foreseeable

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the telecommunications industry preceding the date of the Data Breach.

---

[8] *See Keeping Your Account Secure*, AT&T.com,*https://www.att.com/support/article/myaccount/000101995?bypasscache=1* (last visited April 2, 2024).
[9] *Id.*
[10] *Id.*

41. In light of recent high profile data breaches at other large corporations that collect and maintain voluminous amounts of PII, AT&T knew or should have known that its electronic records and the PII that it stored and maintained would be targeted by cybercriminals and ransomware attack groups.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.

43. Indeed, cyberattacks on telecommunications companies like AT&T have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, potential attack.

Defendant had an Obligation to Protect the PII

44. Defendant's failure to adequately secure Plaintiff's and Class Members' PII breaches duties it owes Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendants also has an implied duty to safeguard its data, independent of any statute.

45. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. S*ee, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

46. Therefore, the increase in such cyber-attacks, and the attendant risk of future cyber-attacks, is and was widely known to anyone in Defendant's industry, including Defendant.

In addition to its obligations under federal and state laws, defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

47. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

48. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained substandard data security systems.

49. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

50. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

51. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

52. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

53. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

54. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

55. Defendant was, or should have been, fully aware of the unique highly sensitive type and the significant volume of data on Defendant's network, amounting to millions of individuals' PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Value of PII

56. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to

$200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

57. Based on the foregoing, the information compromised in the Data Breach, including full names matched with Social Security numbers, is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

58. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[14]

59. The fraudulent activity resulting from the Data Breach may not come to light for years as there may be a time lag between when harm occurs versus when it is discovered, and also between when the PII is stolen and when it is used. According to the U.S. Government

---

[11] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited April 2, 2024).

[12] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited April 2, 2024).

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited April 2, 2024).

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited April 2, 2024).

Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs and damages that would be imposed on Plaintiff and Class Members as a result of a breach.

61. Plaintiff and Class Members now face a lifetime of constant surveillance of their financial and personal records, credit monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

62. Defendant has acknowledged the risk and harm caused to Plaintiff and Class Members as a result of the Data Breach and encouraged Plaintiff and Class Members to remain vigilant by monitoring account activity and credit reports.

Defendant Failed to Properly Protect Plaintiff's and Class Members' PII

63. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

64. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited April 2, 2024).

is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

65. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

67. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for their respective lifetimes.

68. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

[16] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red- flags-rule-how-guide-business (last visited April 2, 2024).

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set ant-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompressionprograms, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[17]

69. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

[17] *Id.* at 3-4.

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[18]

70. Moreover, given that Defendant was collecting, storing, and maintaining the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

71. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

72. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

73. Because Defendant failed to properly protect and safeguard Plaintiff's and Class Members' PII, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

Defendant's Failure to Comply with Industry Standards

74. As shown above, experts studying cyber security routinely identify companies in the Telecommunications industry as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

---

[18] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020). https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a- preventable-disaster/ (last visited April 2, 2024).

75. Several best practices have been identified that at a minimum should be implemented by Telecommunications service providers like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

76. Other best cybersecurity practices that are standard in the telecommunications industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

77. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

78. The foregoing frameworks are existing and applicable industry standards in the telecommunications services industry data storage, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

79. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards.

Defendant's Negligent Acts and Breaches

80. Defendant participated in and controlled the process of gathering the PII from Plaintiff and Class Members in the ordinary course of its business practice.

2. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendant breached these obligations to Plaintiff and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies for its telecommunications services network that would adequately safeguard Plaintiff's and Class Members' PII. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiffs' and Class Members' PII;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of its data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to develop and put into place uniform procedures and data security protections for its network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h. Failing to ensure or otherwise require that it was adhering to one or more of

industry standards for cybersecurity discussed above;

i. Failing to implement or update antivirus and malware protection software in need of security updating;

j. Failing to require encryption or adequate encryption on its data systems;

k. Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' PII provided to Defendant, which in turn allowed cyberthieves to access its IT systems and networks.

Risk of Damages to Plaintiff and Class Members is Present and Ongoing

81. As a result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

82. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution or loss of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

83. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the

data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

84. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

85. Armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on victims.

86. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

87. Thus, due to Defendant's admitted recognition of the actual and imminent risk of identity theft, Defendant has encouraged customers to remain vigilant by monitoring account activity and credit reports and to set up free fraud alerts with the credit bureaus.

88. Plaintiff and Class Members have spent, and will spend additional time in the

future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

Diminution of Value of the PII

89. PII is a valuable property right.[19] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

90. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

91. PII can sell for as much as $363 per record according to the Infosec Institute.[20]

92. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the cybercriminals.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

---

[19] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[20] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited April 2, 2024).

93. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

94. Defendant only encourages Plaintiff and Class Members to remain vigilant by monitoring account activity and credit reports and to sign up for free fraud alerts from nationwide credit bureaus — Equifax, Experian, and TransUnion. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to independently sign up for that service.

95. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

96. There may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

97. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

98. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

breach, where victims can easily cancel or close credit and debit card accounts.[21] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

99. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

Injunctive Relief is Necessary to Protect against Future Data Breaches

100. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected and in compliance with industry standards.

Plaintiff Alison Williamson's Individual Experience

101. At the time of the Data Breach, Defendant retained Plaintiff Williamson's PII in its system.

102. In order to obtain telecommunication services from AT&T, Plaintiff Williamson was required to provide her Private Information to Defendant.

103. As a result of the Data Breach, Plaintiff Williamson has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her financial accounts, implementing extra security on her computers, and resetting automatic billing instructions tied to possible compromised accounts. Plaintiff Williamson has spent significant time

[21] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social- security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited April 2, 2024).

dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

104. Plaintiff Williamson suffered actual injury from having her PII compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of her PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity cost associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect the PII.

105. The Data Breach has caused Plaintiff Williamson to suffer, fear, anxiety, and stress, which has been compounded by the fact that AT&T has still not fully informed her of key details about the Data Breach's occurrence.

106. Plaintiff Williamson anticipates spending considerable time on an ongoing basis to try to mitigate address harms caused by the Data Breach.

107. As a result of the Data Breach, Plaintiff Williamson is at the present and substantial risk and will continue to be at an increased risk of identity theft and fraud for the rest of her life as a direct result of the Data Breach.

108. Plaintiff Williamson has a continuing interest in ensuring that her PII which, on information and belief, remains backed up in AT&T's possession, is protected and safeguarded

from future breaches.

V. CLASS ALLEGATIONS

109. Plaintiff bring this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure.

110. The nationwide class that Plaintiff seeks to represent is defined as follows:

> **All persons in the United States whose Private Information was impacted by AT&T's Data Breach announced on March 30, 2024.**

111. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

112. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, upon information and belief approximately 73 million of individuals' Private Information was comprise in the Data Breah.[22] The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

[22] *See* https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last visited April 2, 2024).

113. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendant learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendant's response to the Data Breach was adequate;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendant owed a duty to Class members to safeguard their Private Information;

h. Whether Defendant breached its duty to Class members to safeguard their Private Information;

i. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

j. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant was unjustly enriched;

n. What damages Plaintiff and Class members suffered as a result of Defendant's misconduct;

o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

114. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

115. Adequacy: Plaintiff is an adequate class representative because her interests do not materially or irreconcilably conflict with the interests of the Class she seeks to represent, she has retained competent counsel, highly experienced in complex class action litigation, and intend to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor her counsel have any interests that are antagonistic to the interests of other members of the Class.

116. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent

or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class)

117. Plaintiff incorporates and reallege all allegations above as if fully set forth herein.

118. Defendant owes a duty of care to protect the Private Information belonging to Plaintiff and Class members. Defendant also owes several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

119. Defendant also owes this duty because industry standards mandate that Defendant protect confidential Private Information.

120. Defendant also owes this duty because it had a special relationship with Plaintiff and Class members. Plaintiff and Class members entrusted their Private Information to Defendant on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendant had the ability to protect its systems and the Private Information stored on them from attack.

121. Defendant also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and the Class. This duty exists to allow Plaintiff and the Class the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

122. Defendant breached its duties to Plaintiff and the Class by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard the Private Information belonging to Plaintiff and Class Members.

123. Defendant also breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class Members that their Private Information had been improperly acquired and/or accessed.

124. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of

time needed to take appropriate measures to avoid unauthorized and fraudulent charges;

- Permanent increased risk of identity theft.

125. Plaintiff and Class members were reasonable and foreseeable victims of any inadequate security practices on the part of Defendant and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

126. In failing to provide prompt and adequate individual notice of the Data Breach, Defendant also acted with reckless disregard for the rights of Plaintiff and Class Members.

127. Plaintiff is entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Nationwide Class)

128. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

129. Section 5 of Plaintiff and the Class entrusted Defendant with their PII.

130. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

131. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

132. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an

unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

133. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

134. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain.

135. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

136. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant, either directly or indirectly, with their confidential PII, a necessary part of obtaining services from Defendant.

137. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

138. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

139. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in

collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

140. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

141. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

142. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

143. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

144. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

145. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

146. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in

protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

147. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

148. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

149. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

150. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII that it was no longer required to retain pursuant to regulations.

151. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

152. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Class would not have been compromised.

153. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

154. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

155. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

156. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

157. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

158. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

159. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present

and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

160. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

161. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

162. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Nationwide Class)

163. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

164. The PII of Plaintiff and Class Members, including full names and Social Security numbers, was provided and entrusted to Defendant.

165. Plaintiff and Class Members provided their PII to Defendant, as part of Defendant's regular business practices in providing telecommunication services.

166. Plaintiff and the Class entrusted their PII to Defendant. In doing so, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen. As a condition of obtaining services and being employed by Defendant's clients, Plaintiff and Class Members provided and entrusted their PII. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

167. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant with the reasonable understanding that their PII would be adequately protected by any business associates, like Defendant, from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiff and Class Members would not have provided their PII.

168. Defendant separately has contractual obligations arising from and/or supported by the consumer facing statements in its Privacy Policy.

169. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

170. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that PII was compromised as a result of the Data Breach.

171. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

172. As a result of Defendant's breach of implied contract, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Nationwide Class)

173. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

174. This count is brought in the alternative to Count III, Breach of Implied Contract.

175. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendant.

176. Defendant was benefitted by the conferral upon it of Plaintiff' and Class Members' Private Information and by its ability to retain and use that information. Defendant understood that it was in fact so benefitted.

177. Defendant also understood and appreciated that Plaintiff' and Class Members' Private Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

178. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class Members would not have provided or authorized their Private Information to be provided to Defendant, and Defendant would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers, gaining the reputational advantages conferred upon it by Plaintiff and Class Members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

179. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

180. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

181. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

182. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

183. Defendant is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically the value to Defendant of the PII and private information that was accessed in the Data Breach and the profits Defendant receives from the use and sale of that information.

184. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

185. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff and the Nationwide Class)

186. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

187. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of the Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

188. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its customers, in particular, to keep secure their PII.

189. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

190. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

191. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

192. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

193. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

194. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and economic and non-economic losses.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in Plaintiff's favor and against Defendant, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit AT&T from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

a. Prohibiting AT&T from engaging in the wrongful and unlawful acts described herein;

b. Requiring AT&T to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. Requiring AT&T to delete, destroy, and purge the PII of Plaintiff's and Class Members' unless AT&T can provide to the Court reasonable justification for the retention and use of such information when weighted against the privacy interests of Plaintiff and Class Members;

d. Requiring AT&T to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. Requiring AT&T to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on AT&T's systems on a periodic basis, and ordering AT&T to promptly correct any problems or issues detected by such third-party security auditors;

f. Requiring AT&T to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring AT&T to audit, test, and train their security personnel regarding any new or modified procedures;

h. Requiring AT&T to segment data by, among other things, creating firewalls and access controls so that if one area of AT&T's network is compromised, hackers cannot gain access to other portions of AT&T's systems;

i. Requiring AT&T to conduct regular database scanning and securing checks;

j. Requiring AT&T to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII , as well as protecting the PII of Plaintiff and Class Members;

k. Requiring AT&T to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

l. Requiring AT&T to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with AT&T's policies, programs and systems for protecting PII;

m. Requiring AT&T to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor AT&T's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

n. Requiring AT&T to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

o. Requiring AT&T to implement logging and monitoring programs sufficient to track traffic to and from AT&T servers; and

p. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis AT&T's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

3. That the Court award Plaintiff and the Class compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by AT&T as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiff be granted the declaratory relief sought herein;

7. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre- and post-judgment interest at the maximum legal rate; and

9. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Date: April 2, 2024

Respectfully Submitted,

/s/ Joe Kendall
Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214-744-3000
jkendall@kendalllawgroup.com

Nathan D. Prosser*
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
(952) 746-2124
nprosser@hjlawfirm.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice application forthcoming*